BAB 12
FIREWALL

Sumber: Elizabeth Zwicky, et.al, *Building Internet Firewalls*, 2nd edition. O'Riley & Associates, 2000.

1. Introduksi

Dalam dunia nyata, firewall adalah dinding (bergerak) yang bisa memisahkan ruangan, sehingga kebakaran pada suatu ruangan tidak menjalar ke ruangan lainnya.

Tapi sebenarnya firewall di Internet lebih seperti parit pertahanan disekeliling benteng, yakni mempertahankan terhadap serangan dari luar.

Gunanya:
- membatasi gerak orang yang masuk ke dalam jaringan internal
- membatasi gerak orang yang keluar dari jaringan internal
- mencegah penyerang mendekati pertahanan yang berlapis

Jadi yang keluar masuk firewall harus acceptable.
Firewall merupakan kombinasi dari router, server, dan software pelengkap yang tepat. Jarang yang berupa box, dan kalaupun dalam bentuk box, harus dikonfigurasikan dengan benar.

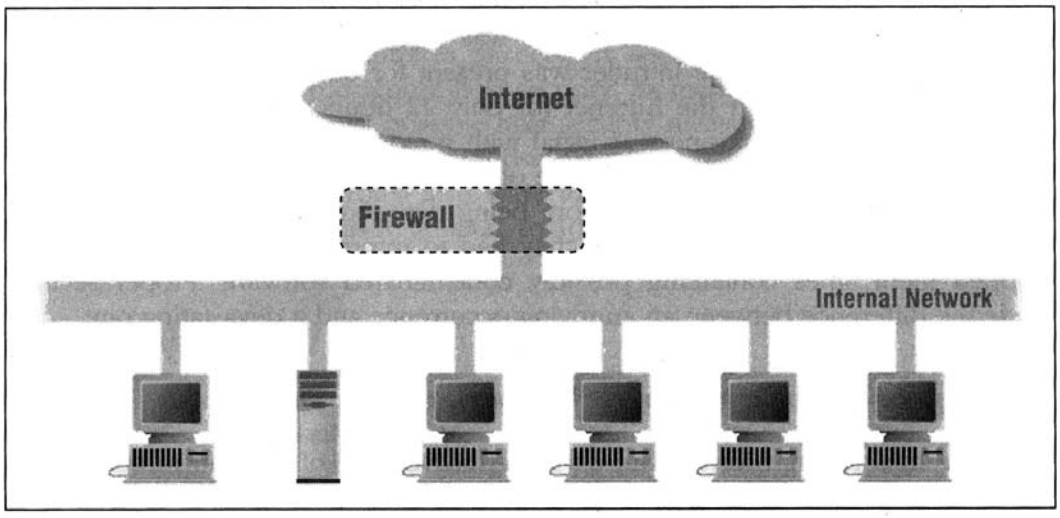

Figure 1-1: A firewall usually separates an internal network from the Internet

Apa yang bisa dilakukan oleh firewall?

1. Firewall adalah *choke point*, yakni pusat “checkpoint sekurit”. Lebih baik memusatkan “keluar masuk” pada satu titik ketimbang harus melakukan pemantai di semua tempat.
2. Firewall bisa memaksakan sekuriti policy. Misalnya jangan sampai ada orang luar yang bisa mengakses directory service dari perusahaan yang berisis arsip pegawai.
3. Firewall bisa mencatat aktifitas Internet dengan efektif, termasuk yang gagal melakukan hacking
4. Firewall bisa membatasi orang lain mengintip-intip jaringan internal, dan kalaupun terhack, maka yang kena hack cuma bagian tertentu saja.

Apa yang tidak dapat dilakukan firewall?

1. Firewall tidak bisa melindungi dari serangan orang dalam
2. Firewall tidak bisa melindungi serangan yang tidak melalui firewall tersebut (tidak melalui chocke point). Misalnya ada yang memasang dial-up service, sehingga jaringan bisa diakses lewat modem.
3. Firewall tidak bisa melindungi jaringan internal terhadap serangan-serangan model baru.
4. Firewall tidak bisa melindungi jaringan terhadap virus.

2. Beberapa prinsip keamanan

1. Least previlage: artinya setiap orang hanya diberi hak akses tidak lebih dari yang dibutuhkan untuk menjalankan tugasnya.
2. Defense in Depth: gunakan berbagai perangkat keamanan untuk saling membackup. Misalnya dapat dipergunakan multiple screening router, sehingga kalau satu dijebol, maka yang satu lagi masih berfungsi.
3. Choke point: semua keluar masuk lewat satu (atau sedikit) gerbang. Syaratnya tidak ada cara lain keluar masuk selain lewat gerbang.
4. Weakest link: “a chain is only as strong as its weakest link”. Oleh karena itu kita harus tahu persis dimana weakest link dalam sistem sekuriti organisasi kita.
5. Fail-Safe Stance: maksudnya kalau suatu perangkat keamanan rusak, maka secara default perangkat tersebut settingnya akan ke setting yang paling aman. Misalnya: kapal selam di Karibia kalau rusak mengapung, kunci elektronik kalau tidak ada power akan unlock, packet filtering kalau rusak akan mencegah semua paket keluar-masuk.
6. Universal participation: semua orang dalam organisasi harus terlibat dalam proses sekuriti.
7. Diversity of Defense: mempergunakan beberapa jenis sistem yang berbeda untuk pertahanan. Maksudnya, kalau penyerang sudah menyerang suatu

jenis sistem pertahanan, maka dia tetap akan perlu belajar sistem jenis lainnya.

8. Simplicity: jangan terlalu kompleks, karena sulit sekali mengetahui salahnya ada di mana kalau sistem terlalu kompleks untuk dipahami.

1. Beberapa Definisi

Firewall:	komponen-komponen yang membatasi akses antara jaringan internal dengan Internet, atau antar-jaringan
Bastion host:	Komputer yang harus dibuat sangat aman dan sering menjadi titik serang karena terbuka di Internet
Dual-homed host:	Komputer yang setidaknya memiliki 2 network interface
Packet filtering:	tindakan untuk menyeleksi arus keluar masuk paket dalam jaringan. Sering disebut screening.
Perimeter network:	jaringan diantara Internet dengan intranet, yang juga sering disebut De-Militerized Zone (DMZ).
Proxy server:	program yang berhubungan dengan server di Internet/extranet, mewakili klien yang ada di dalam intranet.

2. Packet Filtering

Router yang dipergunakan untuk packet filtering disebut screening router.

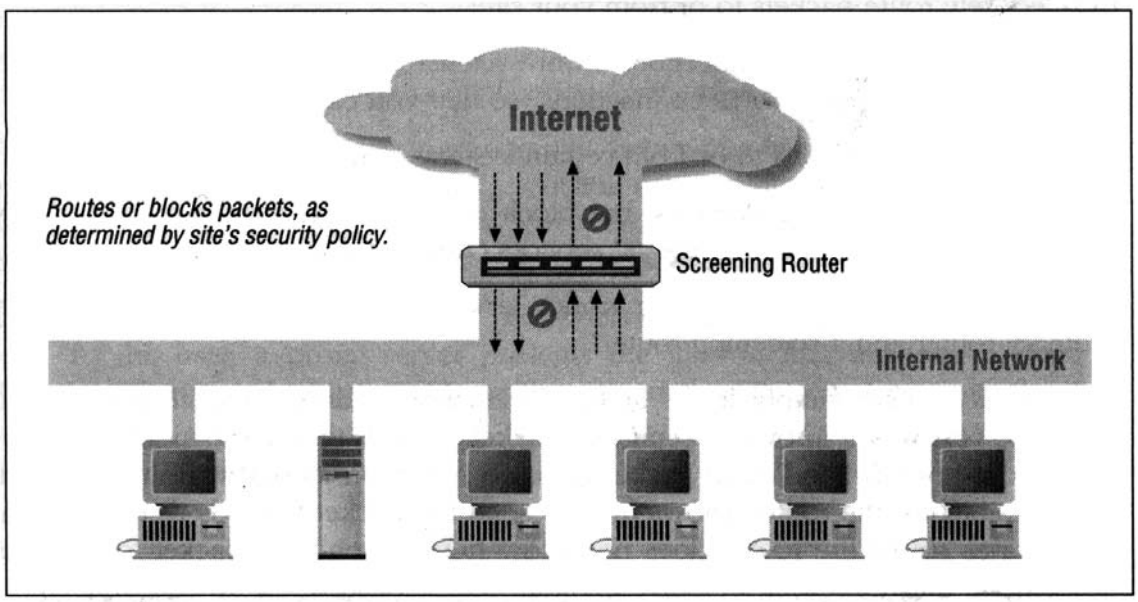

Figure 4–1: Using a screening router to do packet filtering

Yang bisa dijadikan informasi dari paket TCP/IP adalah:

- IP address asal
- IP address tujuan
- Protokol: UDP, TCP atau ICMP

- TCP / UDP port asal
- TCP / UDP port tujuan
- jenis pesan ICMP

Selain itu router juga bisa tahu pada sisi mana paket itu akan keluar atau telah masuk.

Contoh operasi screening router:

a. blok semua akses dari luar ke dalam, kecuali SMPT agar bisa terima e-mail
b. blok semua akses dari dan ke situs yang dipercaya
c. mengizinkan e-mail dan FTP, tetapi tidak mengizinkan rlogin, rsh dsb.

Bedanya screening router dengan router biasa apa?
Screening router selain menentukan kemana sebuah paket dikirim, juga menentukan apakah paket tersebut boleh dikirimkan atau ditolak.

5. Proxy Service

Proxy bisa ditempatkan di dual-homed host atau dalam bastion host dalam firewall. Proxy adalah application-level gateway.

Proxy server membuat ilusi terhadap klien dalam Intranet bahwa sang klien sedang berhubungan langsung dengan server-server di Internet. Sedangkan pada server yang di Internet, seolah-oleh berhubungan dengan user yang sedang bekerja di komputer proxy server.

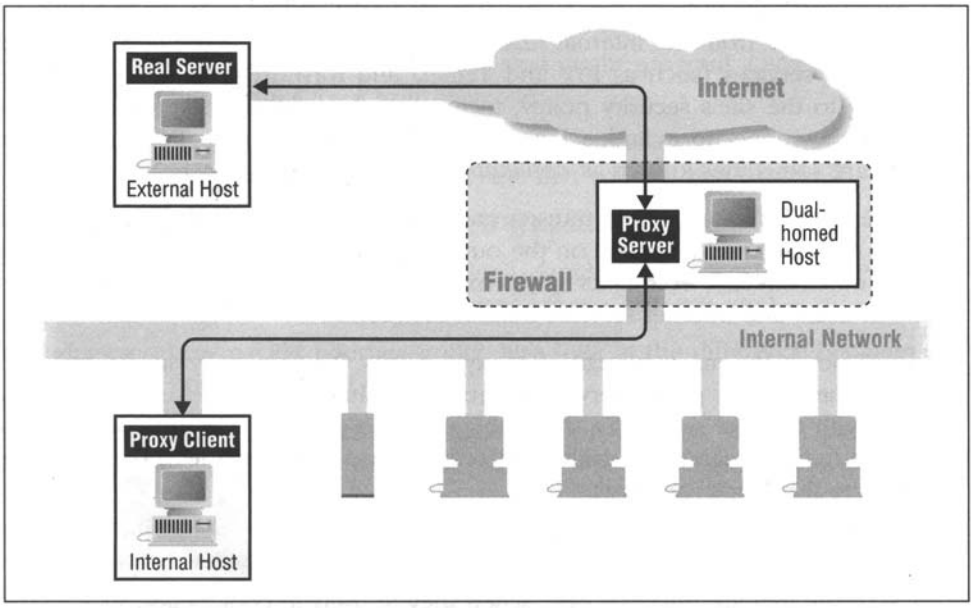

Figure 4–2: Using proxy services with a dual-homed host

Proxy server digunakan bersama-sama dengan mekanisme lain yang mencegah akses langsung klien internal ke host di Internet/extranet. Misalnya: proxy server diletakkan di dual-homed host. Contoh yang paling umum adalah HTTP Proxy server.

3. Arsitektur Firewall

3.1 Dual-homed Host Architecture

Meskipun dual homed host bisa menjadi router, namun untuk menjadi firewall lalu lalu-lintas IP dalam arsitektur ini benar-benar di-blok. Jadi kalau ada paket yang mau keluar masuk, harus lewat proxy.

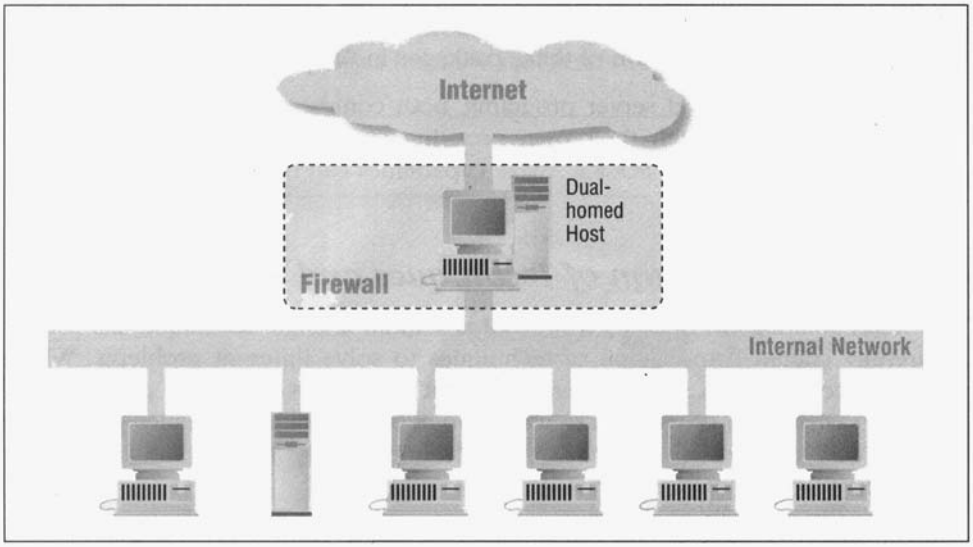

Figure 4–3: Dual-homed host architecture

3.2 Screened Host Architecture

Menggunakan bastion host yang diletakkan dalam intranet, dan seluruh komunikasi keluar masuk harus melalui proxy pada bastion dan kemudian melalui screening router.

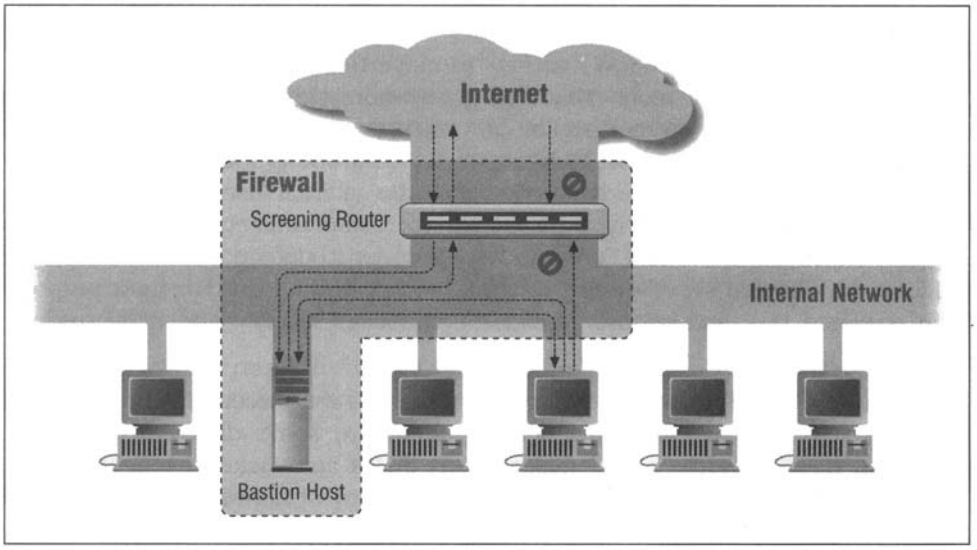

Figure 4–4: Screened host architecture

Sekilas terlihat bahwa dual-homed architecture lebih aman, tetapi dalam prakteknya banyak kegagalan sistem yang memungkinkan paket lewat dari satu sisi ke sisi lainnya dalam dual homed architecture.

Jadi alasan utama menggunakan screened host architecture adalah karena router lebih mudah diamankan ketimbang sebuah komputer/host.

Kejelekan utama kedua-duanya adalah mereka memiliki ‘single point of failure’.

3.3 Screened Subnet Architecture

Apa alasannya? Bastion host sering menjadi target serangan. Jadi idenya adalah kalau bastion host berhasil dibobol, jangan sampai penyerang masuk ke dalam jaringan internal. Oleh karena itu bastion host diletakkan di perimeter network (DMZ).

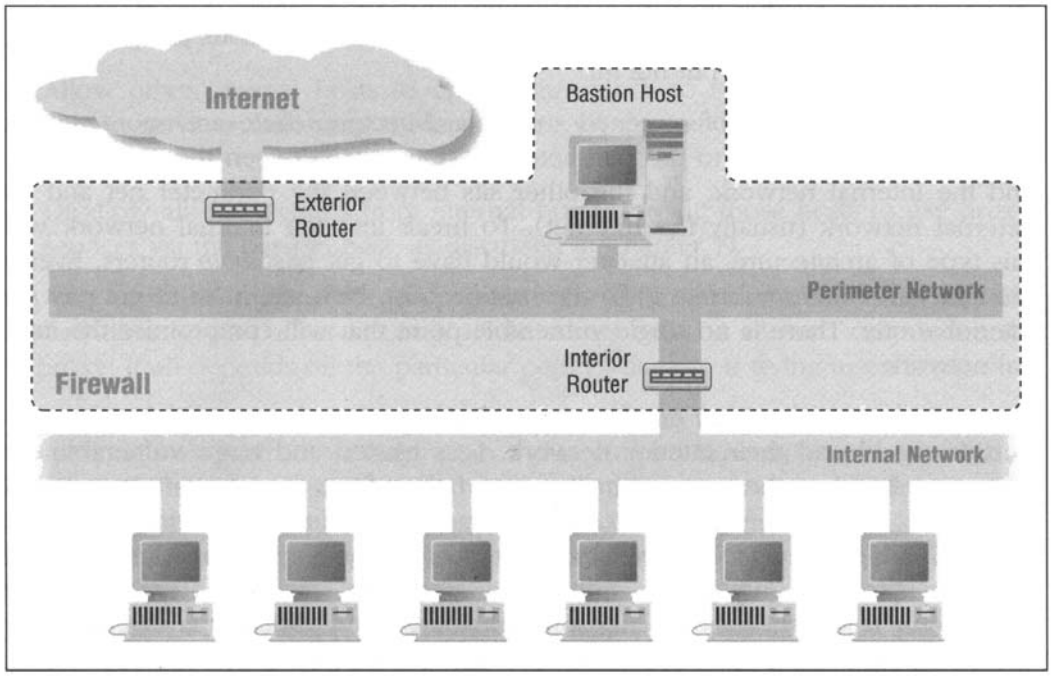

Figure 4–5: Screened subnet architecture (using two routers)

Untuk membobol jaringan, hacker harus menyerang exterior router dan interior router. Ada juga yang memiliki perimeter berlapis, dimana syaratnya agar efektif adalah sistem pertahan tiap lapis harus berbeda-beda.

Perimeter Network

Kalau ada orang yang berhasil menembus ke exterior router dan bastion, maka sang penyerang hanya bisa melihat paket yang berkeliaran di perimeter network saja. Jadi lalu-lintas komunikasi pada jaringan internal (yang relatif sensitif) tidak dapat dilihat oleh penyerang dari perimeter network.

Bastion Host
Bertindak sebagai titik masuk koneksi dari luar, termasuk SMTP, FTP dan DNS.

Sedangkan untuk melakukan koneksi dari client ke server di Internet dapat dilakukan dengan 2 cara:

- mengizinkan router-router agar klien bisa berhubungan dengan server Internet secara langsung
- menggunakan proxy server pada bastion

Interior router (choke router)
Melindungi internal network dari Internet dan perimeter network. Sebaiknya lalu-lintas yang diizinkan antara bastion dengan client, hanyalah yang penting-penting saja. Misalnya hubungan SMTP antara bastion dengan mail server internal.

Perhatikan komputer server internal apa saja yang terhubung dengan bastion, karena itulah yang akan menjadi target serangan jika bastion berhasil dihancurkan oleh hacker.

Exterior router (access router)
Pada prakteknya mengizinkan banyak paket keluar, dan hanya sedikit memfilter paket masuk. Namun, biasanya untuk screening network internal, settingnya sama antara internal dan external router.

Tugas utama external router adalah untuk memblok paket yang memiliki alamat yang palsu dari luar (karena berusaha menyamar dengan alamat IP salah satu host dalam internal network). Karena pasti dari Internet.

Kenapa tidak di internal router? Karena masih bisa dari perimeter net yang sedikit lebih trusted.

4. Variasi Arsitektur Firewall

4.1 Menggunakan Banyak Bastion – OKAY

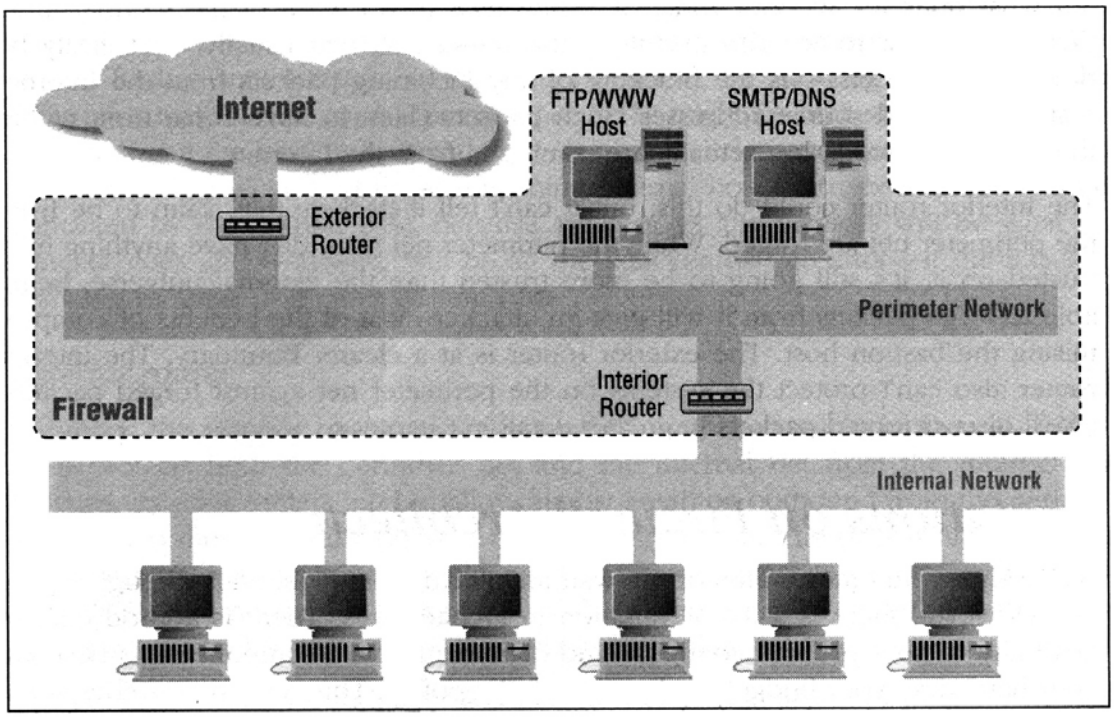

Figure 4-6: Architecture using two bastion hosts

Alasan penggunannya:

- kinerja
- redundancy & backup
- jenis server yang berbeda

Bisa juga bastion yang berbeda untuk menangani ingoing dan outgoing packet.

Bisa juga memisah WWW server dan FTP server dengan maksud agar kalau salah satu berhasil dijebol, maka tetap saja hacker perlu menyerang yang satu lagi.

4.2 Menggabungkan Router Internal dengan Router External - OKAY

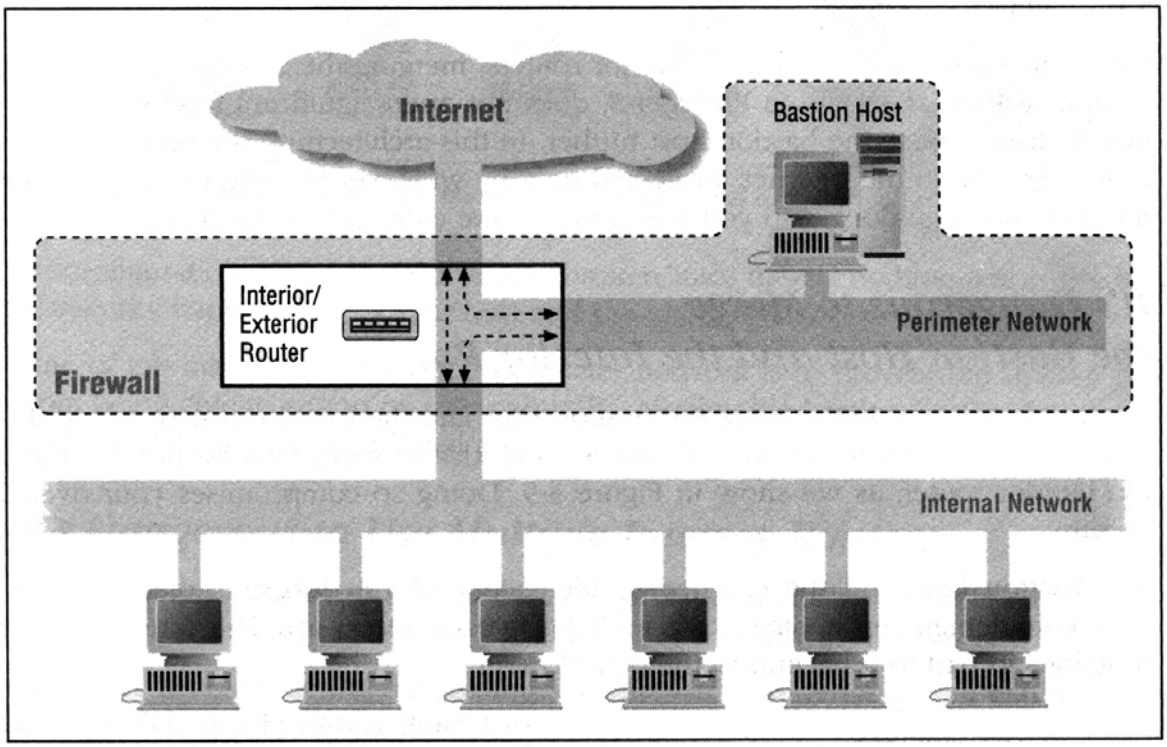

Figure 4–7: Architecture using a merged interior and exterior router

Hanya bisa dilakukan kalau routernya cukup canggih dan fleksibel dan mendukung multiple segment: Internet, perimeter network dan internal network.

Manajemennya lebih mudah, tetapi menyebabkan router itu menjadi single point of failure.

4.3 Menggabungkan Bastion dengan Exterior router – OKAY

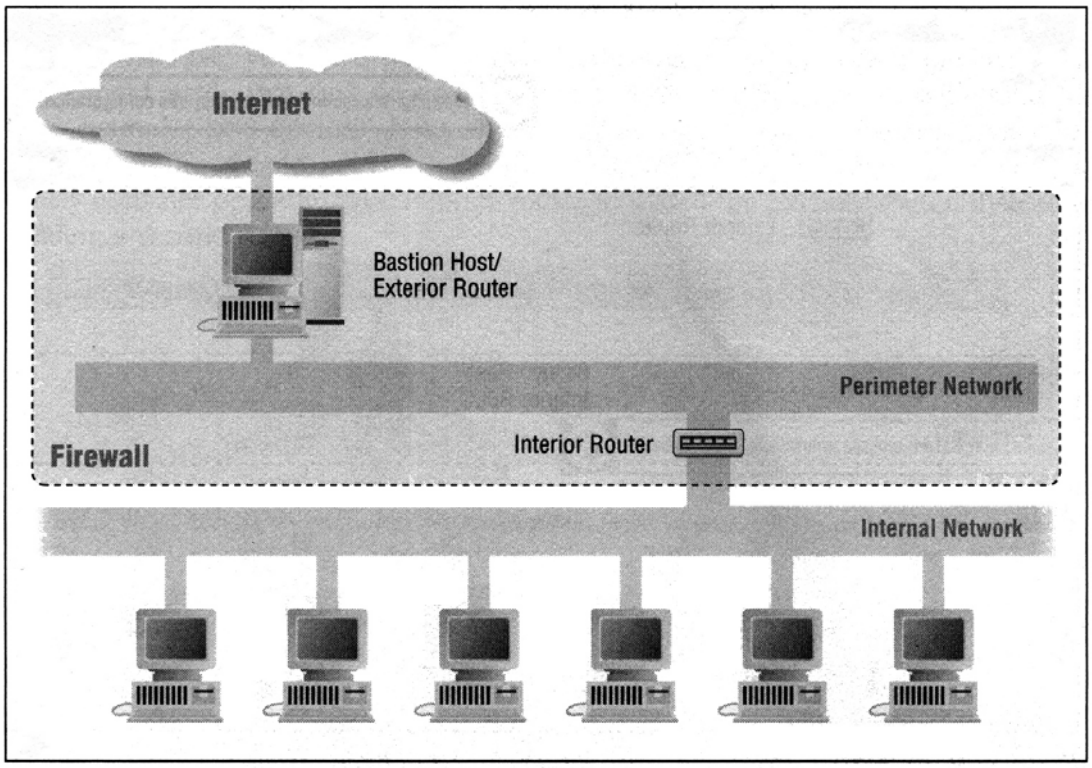

Figure 4–8: Architecture using a merged bastion host and exterior router

Misalnya dalam kasus dimana ada dial-up service. Bastionnya adalah dual-homed host, dan dipasangi server PPP/SLIP. Nah siapapun dari luar yang mengakses bastion akan dianggap sebagai orang asing / Internet.

Kita kemudian bisa juge memasang software router dalam bastion. Memang lambat tetapi mencukupi untuk dial-up service. Kalau bisa software routernya adalah punya kemampuan packet filtering (misalnya Morning Star PPP). Tapi tidak terlalu penting.

Jangan meletakkan dial-up service di dalam jaringan internal (intranet)!

4.4 JANGAN – Menggabungkan Bastion dengan Interior Router

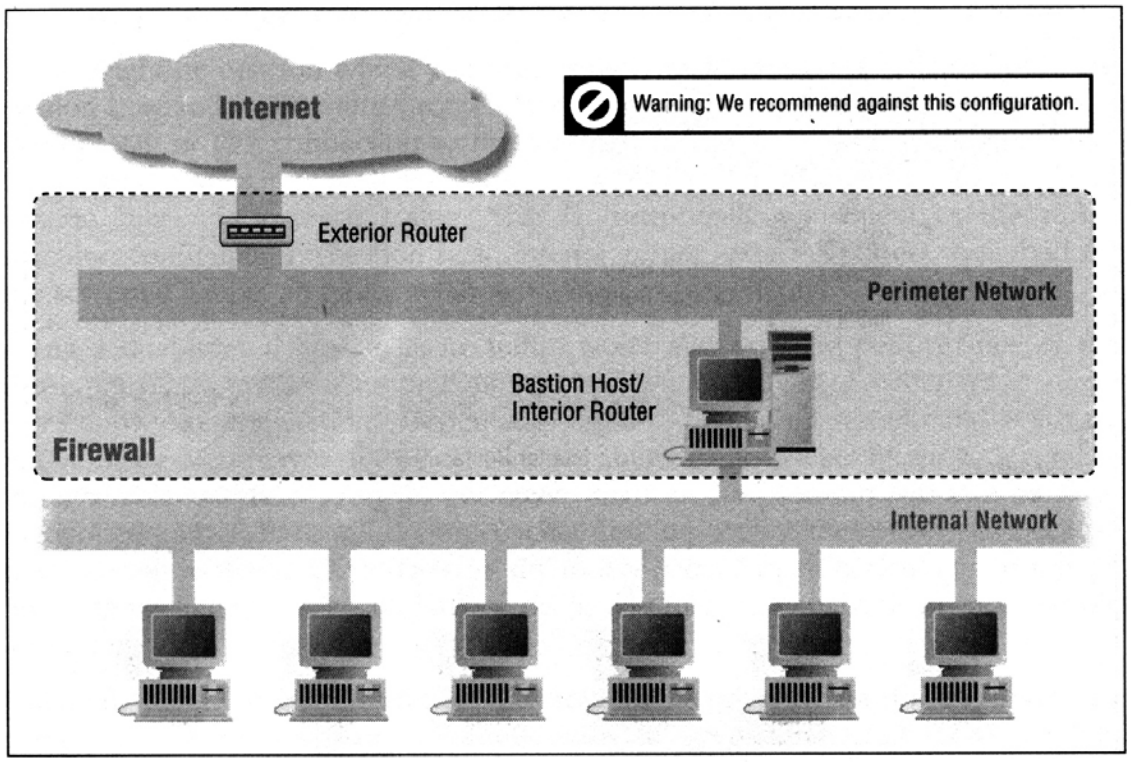

Figure 4–9: Architecture using a merged bastion host and interior router

Extenal router dan bastion melakukan tugas yang berbeda, dan interior router bertugas membackup mereka.

Dalam kasus ini, kita akan memiliki arsitektur screened host firewall. Jika bastion dibobol hacker, maka intranet akan kebobolan juga.

4.5 JANGAN – Menggunakan Multiple Interior Router

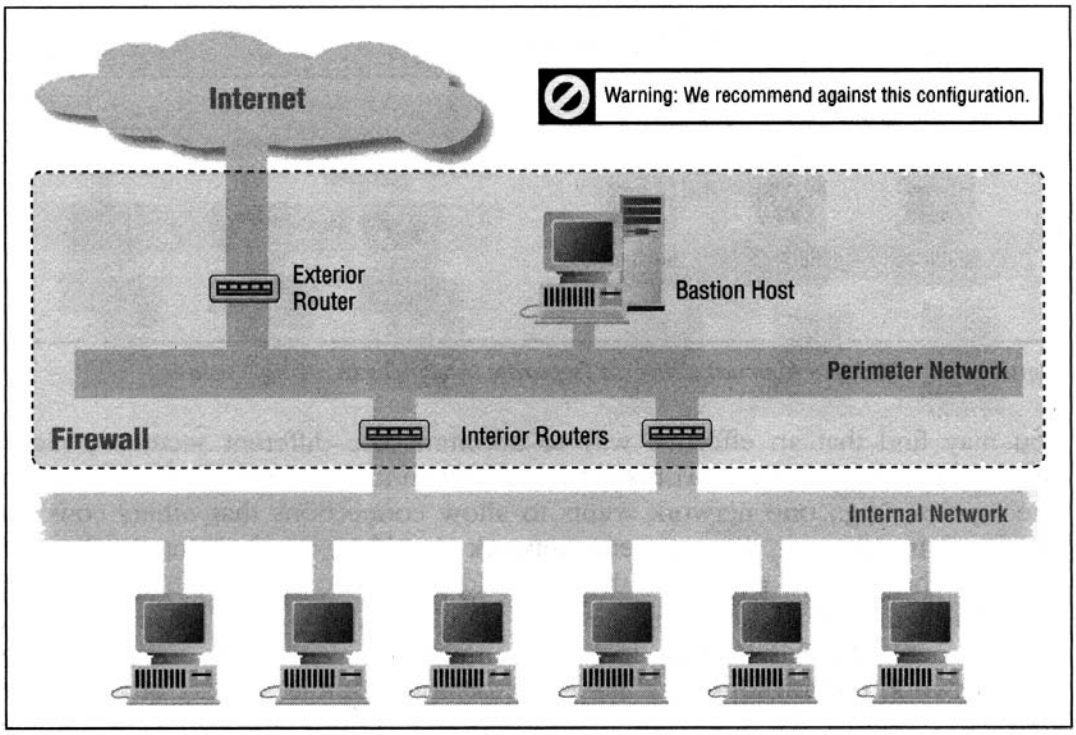

Figure 4–10: Architecture using multiple interior routers

Masalahnya:

- router bisa menduga bahwa cara tercepat untuk mengirimkan paket antar internal host adalah melalui perimeter network, bukan melalui internal network seperti seharusnya. Ini bisa terjadi kalau settingnya ada yang salah.
- sulit menjaga konfigurasi banyak router internal

Konfigurasi yang diperkenankan:

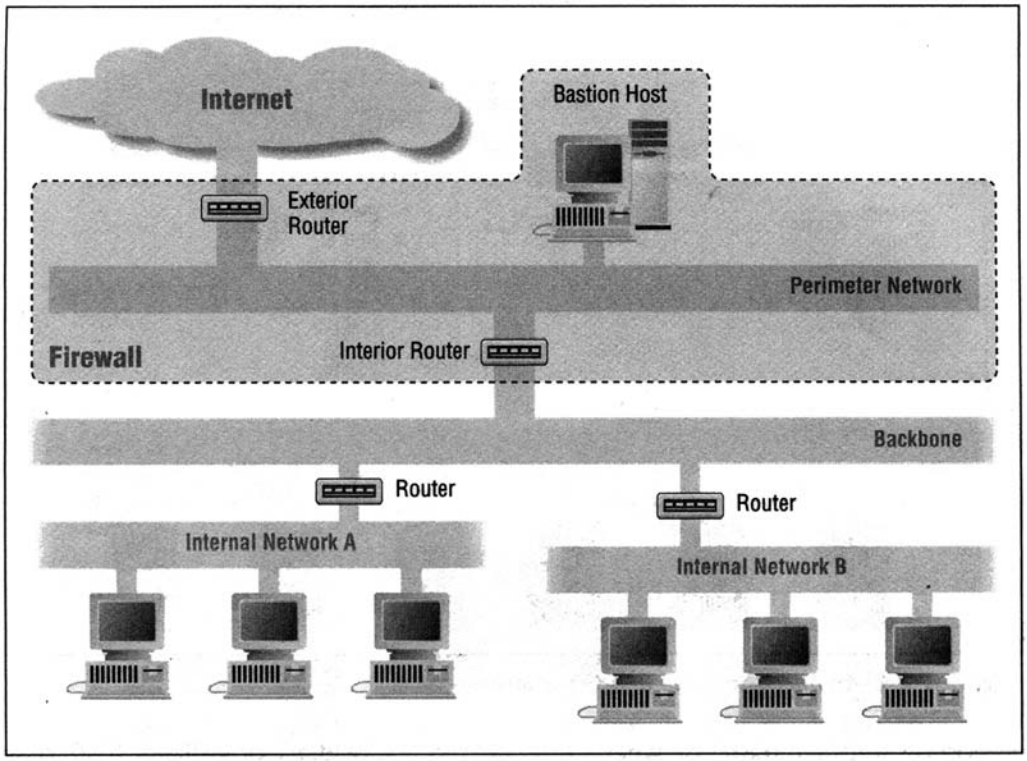

Figure 4–12: Multiple internal networks (backbone architecture)

Konfigutasi untuk multiple segment dalam intranet:

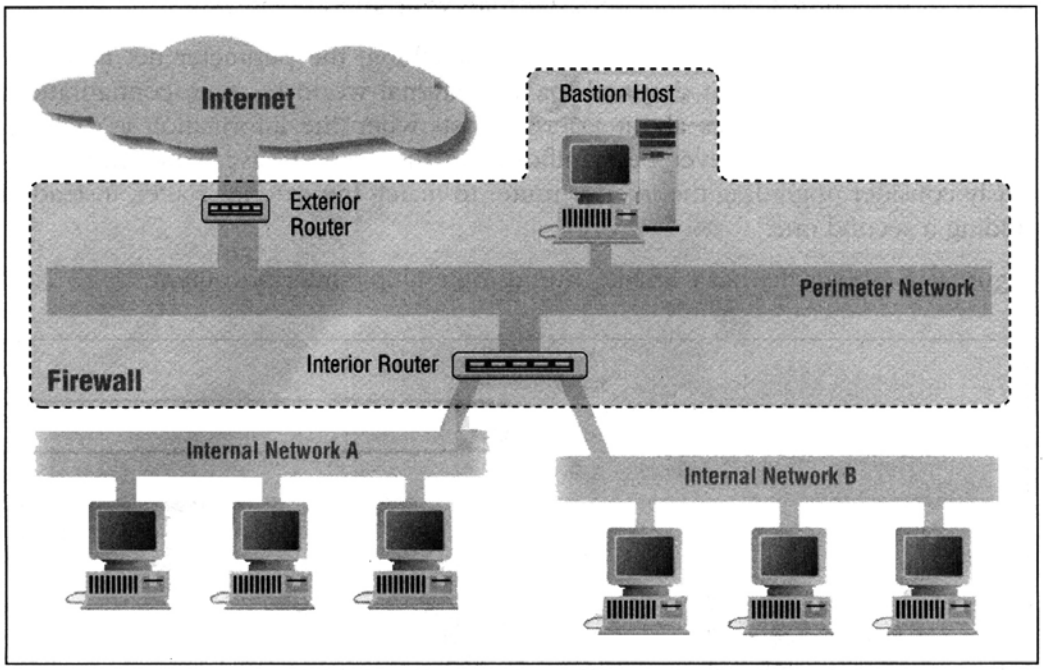

Figure 4–11: Multiple internal networks (separate interfaces in a single router)

4.6 Menggunakan Multiple Exterior Router - OKAY

Penggunaan beberapa router exterior dapat disebabkan karena:

- menggunakan beberapa Internet gateway / service provider untuk redundancy
- ada koneksi ke Internet dan koneksi ke extranet lainnya (misalnya ke supplier).

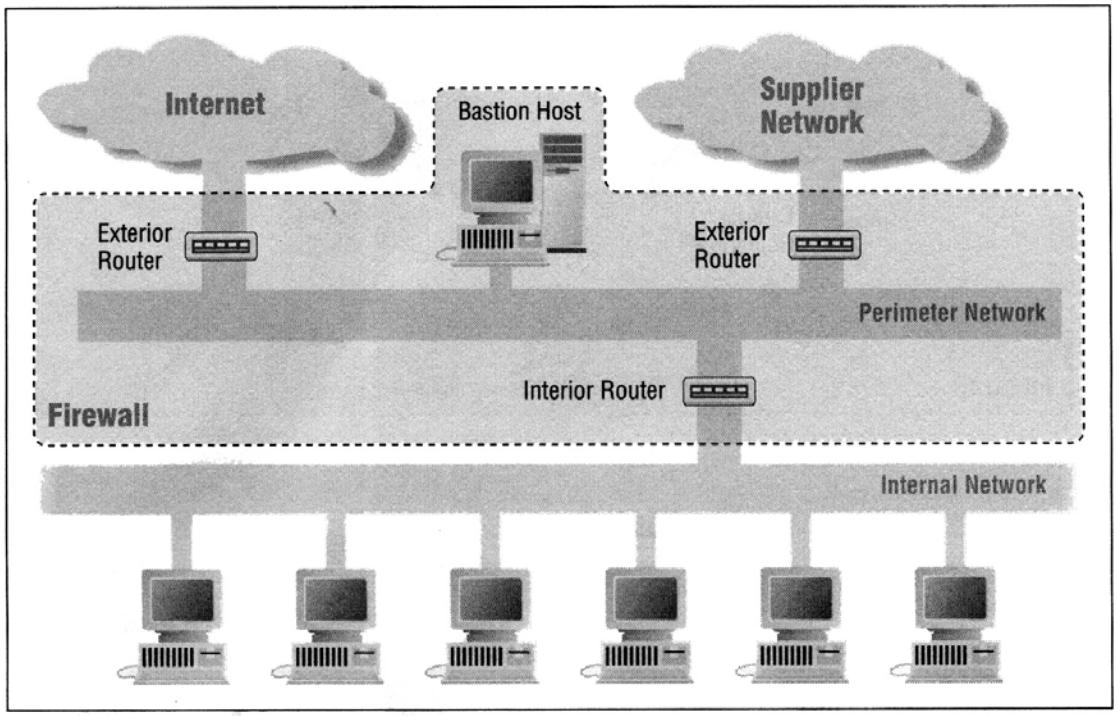

Figure 4–13: Architecture using multiple exterior routers

Tapi kalau ada orang berhasil membobol exterior router yang terhubung ke Internet, maka orang itu akan bisa melihat komunikasi antara kita dengan supplier. Oleh karena itu bisa pakai multiple perimeter network.

4.7 Menggunakan Multiple Perimeter Network – OKAY

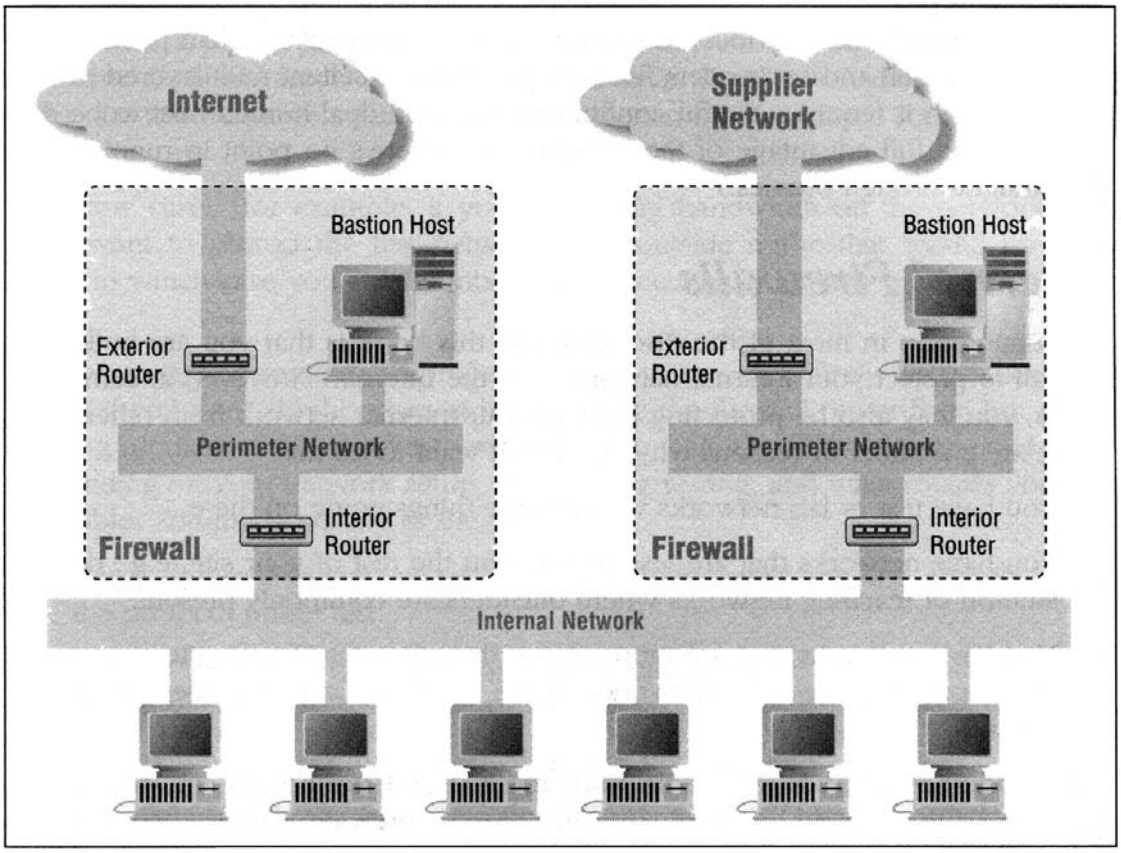

Figure 4–14: Architecture using multiple perimeter nets (multiple firewalls)

Disini kalau perimeter network Internet kebobolan hacker, hacker tetap tidak bisa melihat data yang dipertukarkan antara internal network dengan supplier network.